Confidențialitatea la locul de muncă: Reglementarea camerei de supraveghere video în Dreptul muncii din Ungaria

Adrienn LUKÁCS
Universitatea din Szeged, Ungaria
Universitatea Sorbona din Paris, Franța
lukacs.adrienn@juris.u-szeged.hu

Rezumat: *Lucrarea va examina reglementarea ungară privind protecția vieții private și a datelor referitoare la monitorizarea la locul de muncă, în special în ceea ce privește supravegherea camerei. Ungaria este stat membru al Uniunii Europene, ceea ce înseamnă că trebuie să îndeplinească cerințele legale care decurg din statutul său de membru. Recent, între 2012 și 2014, întregul regulament privind protecția vieții private și a datelor s-a schimbat în Ungaria. Au intrat în vigoare o nouă Constituție, un nou cod civil, un nou cod al muncii și un nou act de protecție a datelor, schimbând extrem de mult mediul juridic al subiectului nostru. Lucrarea va prezenta modul în care Ungaria reglementează supravegherea CCTV în contextul ocupării forței de muncă, din punctul de vedere al protecției datelor, concentrându-se pe mediul juridic și pe practica autorității de supraveghere a protecției datelor cu privire la problema dacă Ungaria îndeplinește cu succes cerințele impuse de Statutul său de membru în Uniunea Europeană. După analiza detaliată a regulamentului și compararea acestuia cu normele UE, am ajuns la concluzia că, urmare a schimbărilor legale, Ungaria se conformează mai bine cerințelor UE, asigurând o protecție eficientă a drepturilor fundamentale ale angajaților. Cu toate acestea, am constatat și câteva insuficiențe ale regulamentului, la care voi propune câteva soluții în lucrarea mea.*

Cuvinte cheie*: dreptul de confidențialitate; legea privind protecția datelor; Codul muncii din Ungaria; supravegherea video la locul de muncă.*

1. Introducere

Există numeroase modalități de monitorizare a angajaților, utilizarea supravegherii video este una dintre ele. Actualitatea subiectului este dată de faptul că în zilele noastre toate tipurile de angajați sunt monitorizați, iar monitorizarea CCTV este o metodă adesea folosită. Problema juridică de bază care apare în timpul acestei practici este aceea că drepturile fundamentale ale angajatului ar putea fi încălcate, și anume, dreptul la viață privată și dreptul la protecția datelor. Aceasta înseamnă, de asemenea, o problemă că, din structura ierarhică a relației de angajare, angajații sunt într-o situație mai dificilă de a proteja aceste drepturi și ar putea avea nevoie de mai multă protecție în timpul aplicării dreptului de monitorizare al angajatorului.

Scopul lucrării mele este de a prezenta reglementarea ungară privind protecția datelor, privind supravegherea camerei la locul de muncă, cu privire la faptul dacă Ungaria îndeplinește cu succes obligațiile ce decurg din statutul de membru al Uniunii Europene. În ultimii ani, am putea experimenta schimbarea completă a mediului juridic în legătură cu subiectul: în 2012 a intrat în vigoare noua Constituție, urmată de un nou Cod al Muncii și un nou act de protecție a datelor. În lucrarea mea voi prezenta aceste reglementări, cele mai importante modificări introduse de aceștia și conformitatea acestora cu legislația UE. În prima parte a lucrării am să prezint regulamentul ungar privind protecția datelor, iar în a doua parte voi examina reglementarea supravegherii camerei și dispozițiile relevante ale Codului Muncii și soluțiile aduse pentru protecția națională a datelor de Autoritatea de supraveghere, respectiv: fostul comisar și - începând cu 2012 - autoritatea.

2. Reglementarea dreptului la confidenţialitate şi dreptul de protecţie a datelor în sistemul juridic maghiar

În zilele noastre, dreptul la intimitate are o importanță crescândă în societățile occidentale. Acest fenomen se datorează dezvoltării rapide a științei și tehnologiei, deoarece acestea au facilitat o posibilă intruziune în sfera privată a individului. Din cauza lipsei de spațiu, nu voi detalia definiția protecției vieții

private și a datelor și relația dintre ele. Fără a oferi o definiție exhaustivă, viața privată poate fi înțeleasă drept "dreptul de a fi lăsat să fie lăsat" [2] sau o aură cvasistă în jurul persoanei care îl separă de lumea exterioară [3] sau "Individul să decidă despre sine" [4]. Dreptul la protecția datelor a apărut după dreptul la intimitate din cauza dezvoltării tehnologice, când reglementările existente privind confidențialitatea nu mai puteau proteja sfera privată a persoanei în vârstă, de fișierele de date computerizate. În hotărârea recunoscută a recensământului populației, Curtea Constituțională Federală Germană a interpretat dreptul la protecția datelor, ca fiind dreptul la autodeterminare informațională. Instanța a afirmat că acest drept permite persoanei să decidă cu privire la divulgarea și utilizarea datelor sale personale, iar această autodeterminare necesită un nivel mai ridicat de protecție în epoca evoluțiilor tehnologice [5]. Acesta a afirmat că, dacă un individ este nesigur în legătură cu datele înregistrate, comportamentul său va fi guvernat de o forță externă; în loc să-și urmeze propriile motivații, el / ea va avea ca scop să se comporte în așa fel încât să nu iasă în evidență de ceilalți [6].

Mai multe organizații internaționale recunosc dreptul la viața privată ca pe un drept fundamental al omului (Organizația Națiunilor Unite: articolul 12 din Declarația Universală a Drepturilor Omului din 1948; articolul 17 din Pactul internațional privind drepturile civile și politice, 1966; Consiliul Europei: articolul 8 din Convenția europeană a drepturilor omului, 1950; Uniunea Europeană: articolul 7 din Carta drepturilor fundamentale a Uniunii Europene, 2000) și dreptul la protecția datelor cu caracter personal (Uniunea Europeană: articolul 8 din Carta drepturilor fundamentale a Uniunea Europeană, 2000).

Din calitatea de membru al Ungariei în aceste organizații internaționale rezultă că Ungaria are obligația de a asigura protecția dreptului la viață privată și a dreptului la protecție a datelor.

În studiul meu mă voi concentra asupra legislației naționale și asupra conformității cu legislația Uniunii Europene. Înainte de a prezenta regulamentul, trebuie să atrag atenția asupra mediului juridic schimbat. Începând cu 1 ianuarie 2012, Constituția a fost înlocuită de Legea fundamentală, Legea privind protecția datelor cu caracter personal și dezvăluirea informațiilor de interes public (Legea LXIII din 1992) a fost înlocuită printr-un nou act de protecție a datelor, Legea privind dreptul la autodeterminare informațională și libertatea de informare (Legea CXII din 2011), iar la 1 iulie 2012 a intrat în vigoare noul Cod al Muncii (Legea I din 2012). De asemenea, trebuie menționat că, în 2014, a intrat în vigoare și noul Cod civil (Legea V din 2013).

Actul fundamental declară protecția dreptului la viață privată și dreptul la protecția datelor, oferind o protecție constituțională acestor drepturi. Codul civil conține dispoziții mai detaliate, dar totuși generale, declarând protecția drepturilor de personalitate și enumerând unele dintre aceste drepturi. Legea privind autodeterminarea informațională și libertatea de informare (denumită în continuare Legea privind protecția vieții private) reglementează în detaliu dispozițiile privind protecția datelor cu caracter personal. Este un act general care se aplică tuturor tipurilor de prelucrare a datelor, deci și procesării care apare în lumea muncii. Nu există un act specific privind examinarea comună a protecției datelor și a supravegherii camerelor la locul de muncă: Codul Muncii conține puține dispoziții speciale privind monitorizarea angajaților, iar Legea privind serviciile de securitate și activitățile anchetatorilor privați (Legea CXXXIII din 2005) conține prevederi în ceea ce privește aplicarea sistemelor electronice de monitorizare.

2.1. Noțiuni de bază privind protecția vieții private din Ungaria: Legea fundamentală și Codul civil

Protecția generală a dreptului la viață privată și dreptul la protecția datelor este asigurată de Legea Fundamentală și Codul Civil. Actul fundamental garantează protecția drepturilor fundamentale. În articolul VI alineatul (1) se prevede că "[i] unii au dreptul la respectarea vieții lor personale și familiale, a domiciliului, a comunicațiilor și a reputației lor", iar la articolul VI subsecțiunea 2 că "[I] unii au dreptul la protecția datelor lor personale, precum și să aibă acces la și să difuzeze informații de interes public". Cu toate acestea, aceste drepturi nu sunt drepturi absolute, ele pot fi limitate prin aplicarea Testului de necesitate și proporționalitate [7]. Curtea Constituțională (denumită în continuare Curtea) a examinat aceste drepturi prin mai multe decizii: prin Decizia nr. 15/1991. (IV.13) [8] a menționat - referindu-se la hotărârea recensământului populației din partea Curții Constituționale Federale germane - că interpretează dreptul la protecția datelor drept dreptul la autodeterminare informațională. Prin Decizia nr. 36/2005. (X.5), Curtea a afirmat că "elementul esențial al dreptului la intimitate este că nici o intruziune sau o înțelegere în sfera

privată a individului nu se va face împotriva voinței sale". Prin Decizia nr. 32/2013. (XI.22), Curtea a examinat dreptul la viață privată și relația sa cu dreptul la demnitatea umană și a declarat protecția extinsă a dreptului la viață privată.

De asemenea, Curtea a examinat supravegherea camerei în mai multe decizii. Prin Decizia nr. 35/2002. (VII.19) a afirmat că, dacă scopul supravegherii video este de a preveni amenințările, numai o amenințare reală și directă poate îndeplini cerințele constituționale ale limitării scopului. În opinia lor, judecătorul Lászó Kiss și judecătorul István Kukorelli și-au exprimat îngrijorarea cu privire la supravegherea camerei și au subliniat că în timpul acestei monitorizări pot fi vizionate și persoane care nu au legătură cu evenimentul monitorizat sau cu scopul lor. De asemenea, se pot întocmi concluziile obținute în sfera privată care nu sunt reluate în scopul monitorizării. Ei au subliniat că monitorizarea poate avea un efect asupra conștiinței și comportamentului individului, deci, chiar dacă camerele pot fi foarte utile, dansatorii reprezentați de ei nu pot fi uitați.

Prin Decizia nr. 36/2005. (X.5), Curtea a examinat utilizarea camerelor de supraveghere pentru protecția proprietății și a declarat că, deși camerele de luat vederi pot constitui un mijloc util de a obține protecția proprietății, ele sunt, de asemenea, capabile să intre în sfera privată a individului și a înregistrării situațiilor sensibile, fără cunoașterea subiectului sau a capacității sale de a evalua consecințele acestor înregistrări. În aceste cazuri nu este numai dreptul la intimitate care ar putea fi încălcat, ci și la dreptul la demnitate umană. Decizia analizează, de asemenea, problema comportamentului implicit și a perioadei de păstrare a înregistrărilor. Judecătorul Kukorelli a explicat, în raționamentul său paralel, că prezența camerelor poate duce la sentimentul de a fi privit în mod constant, ceea ce oferă în mod automat observatorului o poziție de putere. De asemenea, el a atras atenția asupra faptului că protecția proprietății ar putea fi realizată cu mijloace mai puțin invazive (de exemplu, protecție electronică, etichete). El se referă la deciziile anterioare ale Curții, care precizează că vasta cantitate de date conexe - adesea fără conștientizarea persoanei vizate - îl pune pe individ într-o poziție vulnerabilă și duce la o comunicare inegală.

Dreptul la confidențialitate și dreptul la protecția datelor sunt drepturi ale persoanei, care sunt reglementate de Codul civil. Noul nostru Cod civil - care a intrat în vigoare în martie 2014 - prevede, în general, protecția drepturilor persoanei prin faptul că "[i] ea singură are dreptul să-și exercite libertățile personale, în special dreptul la viața privată și la viața de familie, comunicarea cu ceilalți sub orice formă și dreptul la protecție împotriva defăimării, în cadrul legii și în drepturile altora, și să nu se împiedice în exercitarea acestor drepturi de către alții"[Subsecțiunea (1) din Secțiunea 2:43]. Codul civil identifică o listă a drepturilor persoanei, deși protecția juridică este extinsă și la drepturile personale care nu sunt identificate în Codul civil. Printre drepturile specificate referitoare la persoană se numără dreptul la viață privată (care nu a fost specificat în Codul civil anterior) și dreptul la protecție a datelor. În plus, se detaliază mai mult dreptul la asemănarea facială și vocea înregistrată, declarând, ca o regulă generală, că pentru înregistrarea și folosirea asemănării și a vocii este necesar consimțământul persoanei afectate, cu excepția cazurilor de înregistrare a mulțimii sau a unui eveniment public [Subsecțiunile (1) - (2) ale secțiunii 2:48] [9].

2.2. Legea privind confidențialitatea

Rezultă, din calitatea de membru al Ungariei în Uniunea Europeană, că trebuie să respecte cerințele stabilite de UE. În domeniul legislației privind protecția datelor, trebuie menționate două instrumente juridice. Primul dintre acestea este Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (denumită în continuare DPD), care a constituit principalul instrument de protecție a datelor în UE pentru ultimele două decenii. Al doilea document este Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE, care a fost acceptată în aprilie 2016 și a intrat în vigoare în mai 2016. Regulamentul conține câteva reforme importante și va transforma complet modul în care Uniunea Europeană se ocupă de protecția datelor. Având în vedere că scopul acestui studiu este de a prezenta reglementarea efectivă, mă voi concentra asupra directivei DPD, deoarece aceasta este încă aplicabilă până în mai 2018. Articolul 29 al DPD a creat Grupul de lucru pentru protecția datelor, articolul 29, care a adoptat mai multe documente din domeniul protecției datelor și al dreptului muncii, pe care urmează să le discut mai târziu. De asemenea, Curtea de Justiție a Uniunii Europene (denumită în continuare CJUE) are mai multe hotărâri relevante.

Ungaria și-a îndeplinit obligațiile prin transpunerea DPD în Legea privind protecția datelor cu caracter personal și dezvăluirea informațiilor de interes public. Reglementarea ungară privind protecția datelor a fost complet modificată în 2012, când a intrat în vigoare noul act de protecție a datelor. Noul act de protecție a datelor a păstrat câteva dispoziții ale actului vechi [10], însă a introdus o schimbare instituțională semnificativă și a îmbunătățit reglementarea temeiurilor juridice ale prelucrării și a modificat câteva definiții [11]. În această secțiune voi prezenta pe scurt cele mai importante dispoziții, noile schimbări și respectarea de către Ungaria a legislației UE.

În ceea ce privește domeniul de aplicare material, se poate afirma că - în mod similar DPD - Legea privind confidențialitatea este un act general aplicabil tuturor tipurilor de prelucrare a datelor, astfel încât, în absența unei reglementări speciale, acesta să se aplice și procesării datelor referitoare la oameni în dreptul muncii. În ceea ce privește cele mai importante definiții, datele cu caracter personal sunt definite ca "[...] *orice informație referitoare la persoana vizată, în special prin referire la numele său, la un număr de identificare sau la unul sau mai mulți factori specifici fizic, fiziologic, identitatea economică, culturală sau socială, precum și orice referință care rezultă din astfel de informații referitoare la persoana vizată* [.] " [Punctul 2 din secțiunea 3]. Definiția prelucrării datelor (punctul 10 din secțiunea 3) menționează în mod explicit că *fotografierea, înregistrarea video sunt considerate prelucrări de date*, ceea ce face evident că supravegherea camerei este acoperită de legea privind confidențialitatea.

Legea privind protecția vieții private a adus modificări semnificative în ceea ce privește temele juridice ale procesării. Deși actul anterior de protecție a datelor conținea doar două motive legale (consimțământul și autorizarea legii), Legea privind confidențialitatea extinde temeiurile juridice de prelucrare [12]. În timp ce reglementările internaționale reglementează tipurile de relații juridice, în legislația maghiară se pune accentul pe consimțământul și autorizarea legii, deși prin introducerea unor noi motive legale, Legea privind confidențialitatea a făcut un pas spre respectarea DPD [13]. Articolul 7 litera (f) din Directiva DPD definește un temei juridic bazat pe echilibrarea intereselor și a drepturilor părților, ceea ce înseamnă că prelucrarea este legitimă atunci când este necesară pentru respectarea interesului legitim al operatorului sau al terților, cu excepția dacă aceste interese sunt înlăturate de interesele sau de drepturile și libertățile fundamentale ale persoanei vizate. Aceasta este partea reglementării maghiare care diferă de cerințele DPD și face posibilă echilibrarea interesului și a drepturilor, numai dacă obținerea consimțământului persoanei vizate este imposibilă sau prea scumpă [Subsecțiunea (1) a secțiunii 6]. CJUE a declarat într-o decizie din 2011 că articolul 7 litera (f) din DPD are un efect direct [14], astfel că din această decizie rezultă că regulamentul ungar nu respectă dispozițiile UE și ar fi nevoie de o modificare a legii.

Consimțământ "înseamnă orice indicație specifică și în cunoștință de cauză exprimată în mod expres și în cunoștință de cauză a dorințelor sale, prin care persoana vizată își exprimă acordul cu privire la prelucrarea datelor cu caracter personal referitoare la acesta fără limitare sau în legătură cu operațiuni specifice [.]" (Punctul 7 din secțiunea 3). Nu trebuie uitat că în relația de angajare, în care se poate găsi o relație ierarhică între angajator și angajat, natura voluntară a consimțământului poate fi pusă la îndoială [15].

În mod similar cu reglementările internaționale, regulamentul ungar definește și principiile de bază ale prelucrării. *Principiul limitării scopului* a fost definit pentru prima dată în Ungaria în decizia din 15/1991. (IV.13) al Curții Constituționale [16]. Conform acestei decizii, orice prelucrare trebuie să aibă, în fiecare etapă a prelucrării, un scop legitim, specific și explicit [Subsecțiunea (1) din secțiunea 4]. În legătură cu acest principiu, trebuie menționat *principiul necesității*. Acest principiu înseamnă că numai datele personale esențiale și potrivite pentru acest scop vor fi prelucrate [Subsecțiunea (2) a secțiunii 4]. Dacă există o metodă mai puțin intruzivă, se folosește această metodă. Procesarea fără scop și necesitate este ilegitimă, chiar dacă se bazează pe consimțământul persoanei vizate [17]. Aceasta înseamnă că angajatorul nu poate monitoriza continuu angajații, fără un scop explicit, chiar dacă a obținut consimțământul angajaților. Angajatorul poate folosi aparatele de fotografiat numai în perioadele și cu metode esențiale, pentru scopul prelucrării. Prelucrarea este, de asemenea, legală și corectă, iar precizia, completitudinea și actualizarea datelor trebuie să fie garantate. De asemenea, Legea privind confidențialitatea menționează printre principii cerința de identificare a persoanei vizate [Subsecțiunile (3) - (5) din secțiunea 4].

Legea privind confidențialitatea conține dispoziții privind securitatea datelor, condițiile de transmitere transfrontalieră a datelor cu caracter personal, drepturile individului (dreptul de a fi informat, de a rectifica, de a șterge, de a bloca), de informația preliminară și de executarea judiciară a acestor drepturi [18].

În opinia mea, regulamentul ungar privind protecția datelor respectă regulamentul UE, cu excepția temeiurilor legale ale prelucrării. Pentru a obține o respectare deplină, ar fi necesar un amendament, ceea ce înseamnă că, la sfârșitul formulării temeiului juridic de echilibrare a intereselor, condițiile de consimțământ imposibil sau prea scump ar trebui să fie șterse.

În conformitate cu DPD, toate statele membre furnizează o autoritate independentă pentru protecția datelor, responsabilă de monitorizarea aplicării DPD (articolul 28 din DPD). În Ungaria, în 2012, nu s-a schimbat doar mediul juridic, ci și sistemul instituțional de protecție a datelor: la 1 ianuarie 2012 a fost reziliată instituția actualului comisar pentru protecția datelor (denumit în continuare "comisar") și a fost înlocuită de Autoritatea Națională pentru Protecția datelor și libertatea de informare (denumită în continuare "Autoritatea"). În ceea ce privește această schimbare instituțională, CJEU a condamnat Ungaria pentru neîndeplinirea obligațiilor sale, deoarece, la momentul creării Autorității, mandatul comisarului nu a expirat. Instituția comisarului a fost reziliată și acesta nu a fost desemnat ca președinte al Autorității. În acest sens, Ungaria a încălcat cerința de a furniza o autoritate națională independentă, prevăzută la articolul 28 alineatul (1) din DPD [19].

2.3. Noul Cod al Muncii

După cum am menționat mai sus, în 2012 a intrat în vigoare un nou Cod al Muncii, care a adus schimbări fundamentale în viața privată la locul de muncă, pe care îl voi prezenta în această secțiune. Codul anterior al muncii (Actul XXII din 1992) conținea doar dispoziții foarte scurte privind confidențialitatea și protecția datelor la locul de muncă. Aceasta a constat doar în două dispoziții, menționând în secțiunea 77 alineatul (1) că "*un angajat nu poate fi solicitat decât să facă o declarație, să completeze o fișă tehnică sau să dea un test de aptitudini care să nu încalce drepturile fundamentale și care furnizează, în esență, informații de fond privind aspectele legate de stabilirea unui raport de muncă* [...]", iar în secțiunea 3 subsecțiunea 4, potrivit căruia "[...] *angajatorii pot să dezvăluie doar fapte, date și opinii referitoare la un angajat, către terțe persoane, în cazurile prevăzute de lege sau cu consimțământul angajatului*" [20].

Contrar reglementării anterioare, secțiunile 9-11 din Codul Muncii afișează protecția drepturilor referitoare la personalitate și conțin dispoziții privind protecția datelor și monitorizarea angajaților. Secțiunea 9 prevede că pentru drepturile personale ale angajatorului și angajatului se aplică dispozițiile Codului civil și se precizează că, deoarece aceste drepturi nu sunt absolute, restricția lor ar putea fi posibilă. Această restricție are două condiții: *trebuie să fie direct legată de scopul relației de angajare și proporțională cu obiectivul acesteia*. Motivul direct legat de scopul raportului de muncă include cazuri în care angajatorul nu ar putea să-și îndeplinească obligațiile care decurg din raportul de muncă, fără a limita drepturile persoanei. În ceea ce privește proporționalitatea, obiectivul angajatorului și dezavantajul angajatului trebuie să fie echilibrate [21]. Angajatul nu poate renunța, în general, la drepturile sale personale, iar orice declarație referitoare la aceste drepturi va fi dată numai în scris [Subsecțiunea (3) din secțiunea 9].

Secțiunea 10 din Codul muncii conține mai multe dispoziții specifice referitoare la declarația salariatului, care prevede că "unui lucrător i se poate solicita să facă o declarație sau să dezvăluie anumite informații numai dacă nu încalcă drepturile sale legate personale și dacă se consideră necesar la încheierea sau încetarea raportului de muncă". În timpul raportului de muncă, angajatorul obține o mulțime de informații și date referitoare la angajat, iar prelucrarea acestor date trebuie să respecte cerințele stabilite în Legea privind protecția vieții private [22]. În ceea ce privește testele de aptitudini, Codul muncii prevede că numai un regulament privind angajarea poate prescrie un test de aptitudini sau că testul este necesar pentru a explica drepturile și a îndeplini obligațiile, în conformitate cu reglementările privind ocuparea forței de muncă [Subsecțiunile (2) - (4) ale secțiunii 10].

Codul muncii are acum dispoziții care reglementează problema monitorizării angajaților. Din dreptul angajatorului de a monitoriza, rezultă că acesta are dreptul (chiar și o obligație) de a monitoriza dacă angajații respectă ordinele, angajatorul nu are doar un drept, ci și obligația de a asigura ordinea și disciplina la locul de muncă [23]. Angajatul poate fi monitorizat numai în legătură cu munca, limitată de dreptul său la demnitate și viața privată, deoarece nu poate constitui obiectul monitorizării [Subsecțiunea (1) din secțiunea 11]. Angajatorul are obligația de a informa salariații cu privire la restricționarea drepturilor personale, prelucrarea datelor cu caracter personal și monitorizarea angajaților [Subsecțiuni (2) ale secțiunilor 9, 10, 11].

Toate acestea înseamnă că angajatorul are dreptul de a utiliza camera de supraveghere pentru a monitoriza angajații, deși acest drept are restricții, deoarece trebuie să respecte drepturile personale ale angajatului. În ciuda Codului muncii care conține dispoziții privind monitorizarea angajaților, actul nu oferă nicio indicație cu privire la măsura în care camerele pot fi utilizate, și cum să se realizeze echilibrul dintre interesele angajatorului și drepturile angajaților. Prin urmare, este esențial să examinăm practica comisarului și a autorității.

2.4. Legea privind serviciile de securitate și activitățile anchetatorilor privați

Secțiunile 30 și 31 din Legea privind serviciile de securitate și activitățile anchetatorilor privați conțin reglementări disproporționate cu privire la utilizarea camerei de supraveghere. În același timp, aceste dispoziții se aplică, în general, monitorizării electronice efectuate de polițiști și nu în special monitorizării rezultate din contextul angajării. Potrivit actului normativ, gardianul poate opera un sistem electronic de monitorizare numai pentru a asigura serviciile de securitate, dar trebuie să respecte dispozițiile prezentului act normativ și regulamentul de protecție a datelor prevăzute de Legea privind protecția vieții private [Subsecțiunea (1) din Secțiunea 30]. Garda poate opera sistemul de monitorizare numai în zone private sau în zone deschise publicului, cu condiția ca persoanele în cauză să-și fi dat acordul pentru monitorizare [Subsecțiunea (2) din Secțiunea 30]. Monitorizarea nu poate fi efectuată în zone în care ar aduce atingere dreptului la demnitate umană (de ex. în vestiare sau în baie) [Subsecțiunea (3) din Secțiunea 30].

Scopul sistemelor electronice de monitorizare (cele care înregistrează imaginile) poate fi protejarea vieții omului și a integrității fizice, a libertății personale, păstrarea sigură a substanțelor periculoase, protejarea secretelor de afaceri, a plăților, a băncilor și a valorilor mobiliare și protecția proprietății. Pe lângă existența unuia dintre aceste scopuri, este de asemenea necesar ca circumstanțele să facă posibilă descoperirea și prevenirea faptelor infracționale, precum și flagrantul pentru prinderea făptuitorului. Aplicarea dispozitivelor de monitorizare ar trebui să fie limitată într-o măsură necesară, și nu poate restrânge disproporțional dreptul la autodeterminare informațională [Subsecțiunea (1) din Secțiunea 31]. Ca regulă generală, imaginile înregistrate nu pot fi păstrate mai mult de 3 zile lucrătoare [Subsecțiunea (2) din Secțiunea 31], dar actul conține mai multe excepții.

În ceea ce privește accesul la înregistrări, actul normativ stipulează că numai persoana care desfășoară activitatea de securitate are dreptul de a accesa imaginile, și că este necesar pentru îndeplinirea obligațiilor care îi revin în temeiul contractului sau pentru prevenirea sau întreruperea încălcării comise de făptuitor [Subsecțiunea (7) din Secțiunea 31].

În concluzie, se poate spune că, odată cu intrarea în vigoare a noului cadru legislativ, au fost introduse schimbări semnificative, în special în noul Cod al Muncii și în Legea privind protecția vieții private. Cu toate că Legea privind protecția vieții private a făcut pași importanți în vederea respectării legislației UE și asigură un nivel adecvat de protecție a datelor, iar Codul Muncii conține dispoziții privind protecția datelor, nu există niciun alt act normativ care să reglementeze problema camerei de supraveghere la locul de muncă. Din lipsa lex specialisului și din natura generală a regulamentului existent, rezultă că este esențial să se examineze în detaliu practica Comisarului și a Autorității, pentru a putea răspunde la întrebarea: în ce condiții este posibil astăzi Să folosească supravegherea CCTV a angajaților în Ungaria?

3. Camera de supraveghere video

3.1. Ascensiunea supravegherii cu ajutorul camerei video la locul de muncă

Monitorizarea CCTV s-a răspândit în anii 1970 și de atunci a înregistrat progrese enorme. Camerele de supraveghere au devenit tot mai mici, mai ieftine și mai accesibile, toate companiile contribuind la proliferarea lor. În prezent, ele înregistrează practic toate mișcările pe care le facem: sunt prezente pe scări, pe străzi, în centre comerciale, în bănci, în instituții de învățământ, pe vehicule de transport public, în parcări, pe aeroporturi, etc. Proliferarea lor era în principiu justificată prin necesitatea asigurării protecției proprietății și a indivizilor [24].

Deși pot fi utile în atingerea obiectivelor lor, în multe cazuri sa demonstrat opusul [25].

În lucrarea mea nu voi prezenta aceste avantaje și dezavantaje tehnologice, mă voi concentra asupra examinării problemelor legale care apar din utilizarea camerei de supraveghere.

Lumea muncii nu constituie o excepție de la răspândirea camerei de supraveghere; tot mai mulți angajatori folosesc diferite tehnici de monitorizare, cum ar fi supravegherea CCTV pentru monitorizarea angajaților [26]. În timp ce scopul inițial al aparatelor foto era de a asigura securitatea, angajatorii consideră că este foarte tentant să folosească sistemul CCTV pentru a monitoriza munca angajaților din diferite motive. În timpul existenței relației de muncă, angajatorul este interesat de monitorizarea lucrătorilor - de exemplu prin intermediul supravegherii video - pentru a-și asigura interesele economice legale, care au mai multe dimensiuni.

O dimensiune a interesului angajatorului este controlul efectuării muncii. În acest domeniu, angajatorul are dreptul de a asigura o gestionare eficientă. Ca urmare a naturii contractului de muncă, angajatorul are dreptul să monitorizeze dacă angajatul își îndeplinește sarcinile și își îndeplinește îndatoririle în mod corect. Mai mult, el / ea este interesat să asigure productivitatea și profitabilitatea. Prin urmare, este o afirmație firească din partea angajatorului, de a obține suficiente informații despre lucrători pentru a se asigura că angajatul lucrează cu adevărat, își desfășoară munca într-o manieră eficientă și este cel mai bun care ar putea fi angajat [27]. Acesta este motivul pentru care angajatorul este interesat de obținerea de informații privind performanța muncii, deoarece, cunoscând aceste informații, poate organiza munca într-un mod mai eficient, prin aplicarea metodelor și a tehnologiilor care pot crește productivitatea.

O altă dimensiune este protecția proprietății și a persoanelor. Angajatorul este responsabil pentru asigurarea siguranței angajaților prin asigurarea unui mediu de lucru adecvat [28]. Astfel, este evident că este interesat să monitorizeze dacă angajații respectă regulamentele de securitate la locul de muncă, iar monitorizarea CCTV este adecvată pentru a furniza acest tip de informații. Mai mult, angajatorul este, de asemenea, interesat de prevenirea infracțiunilor comise la locul de muncă [29]. Poate fi o infracțiune sau un act împotriva angajatorului (de exemplu, furtul, provocarea de daune) sau împotriva angajatului (de exemplu, vătămări corporale, viol). Aceste acte devin detectabile sau chiar previzibile prin monitorizarea CCTV.

Examinând întrebarea din punct de vedere juridic, se poate spune că părțile din relația de angajare au diferite drepturi și obligații. Interacțiunea dintre aceste drepturi și obligații poate fi văzută astfel încât: ceea ce este un drept pe de o parte va fi o obligație din partea cealaltă [30]. Interesul angajatorului de a restrânge drepturile personale ale salariaților, subliniază consolidarea acestor drepturi și obligații [31]. Angajatorul are obligația de a asigura protecția angajaților, obligație care apare ca drept al angajatului și ca obligație de muncă. Angajatorul este îndreptățit și, în același timp obligat, să dea instrucțiuni și să monitorizeze în legătură cu munca, iar în timpul acesta, angajatul are dreptul la protecția datelor, dar are și obligația de a respecta legitimitatea angajatorului – interesele fiind colective [32]. Angajatorul este obligat să asigure securitatea și sănătatea lucrătorilor. Pe de o parte, angajatul are dreptul să solicite acest lucru și, pe de altă parte, are și obligația de a asigura protecția [33]. Ambele părți au interes în consolidarea acestor drepturi și obligații, iar supravegherea cu ajutorul camerelor poate contribui la punerea lor în aplicare.

Există drepturi fundamentale și interese semnificative de ambele părți, astfel încât trebuie să se găsească și să se respecte un echilibru între punerea în aplicare a acestora în timpul elaborării reglementărilor și al aplicării monitorizării [34]. În același timp, monitorizarea nu poate fi nelimitată, deoarece angajatul este și o ființă umană la locul de muncă, așa că - deși angajatorul plătește în schimbul muncii angajatului - drepturile sale personale vor fi repetate la locul de muncă [35]. Există, de asemenea, o trăsătură specifică privind dreptul la viață privată și dreptul la protecție a datelor, în contextul ocupării forței de muncă, deoarece există o relație ierarhică între angajator și salariat, care face ca angajații să se afle într-o poziție mai vulnerabilă. Acest aspect nu trebuie uitat în timpul elaborării regulamentului. În paralel cu vulnerabilitatea angajatului, trebuie să menționăm și vulnerabilitatea angajatorului, deoarece, datorită progresului tehnologic și al informaticii, posibila abuzare a datelor și secretelor de afaceri ale angajatorului este mai ușoară, cauzând un prejudiciu uriaș angajatorului [36].

3.2. Practica fostului Comisar

Jurisprudența maghiară nu conține multe cazuri în ceea ce privește supravegherea cu ajutorul camerei; acele câteva verdicte în care erau implicate camere de supraveghere, au fost utilizate ca dovadă, angajatul nu a evocat încălcarea dreptului la autodeterminare informațională [37]. Putem să învățăm despre

cazurile relevante din practica Comisarului și din 2012 - când această instituție a fost înlocuită - din practica Autorității. Aceste două instituții au dezvoltat o bogată "jurisprudență" în decursul celor aproape două decenii de existență, elaborând treptat principiile aplicabile supravegherii încăperii de lucru și creând o recomandare-cheie în acest domeniu.

Comisarul a examinat subiectul camerei de supraveghere în diverse cazuri. Comisarul a experimentat un număr din ce în ce mai mare de cazuri, astfel încât în anul 2000 a publicat o recomandare intitulată "Recomandarea Comisarului pentru protecția datelor cu privire la dispozitivele de înregistrare și stocare video operate în scopul monitorizării și colectării datelor" (numărul dosarului 475 / H / 2000). Recomandarea s-a referit la problemele de confidențialitate în general, implicând și domeniul dreptului muncii. În acest document, Comisarul a atras atenția asupra faptului că, în cazul lipsei reglementării sectoriale, se aplică regulamentul general privind protecția datelor. Acesta a subliniat cerința principiului limitării scopului, subliniind că, deși unele interese ar putea fi foarte semnificative, nu trebuie uitat că supravegherea cu camera de filmare limitează un drept constituțional fundamental. Prin urmare, este esențial să se respecte garanțiile legale prevăzute în Legea privind protecția vieții private. O orientare din 2001 (numărul cazului: 636 / H / 2001) este legată de această recomandare și atrage, de asemenea, atenția asupra faptului că în perioadele în care nu există o reglementare sectorială și știința și tehnologia se dezvoltă mai repede Legea ar putea reacționa la aceste schimbări, comportamentul oamenilor, moralul și principiile fundamentale juridice inspirate de aceste valori ar trebui să devină mai importante.

În 2005, Comisarul a emis o rezoluție (numărul cazului: 284 / A / 2005) subliniind importanța temeiurilor juridice ale prelucrării și - în ceea ce privește principiul limitării scopului - semnificația și rolul testului în protejarea drepturilor fundamentale stabilite de Curtea Constituțională. De asemenea, Comisarul a abordat și problema camerei de supraveghere în mai multe cazuri practice. Într-o altă rezoluție din 2005 (numărul cazului: 1165 / K / 2005-3.), el a declarat că, camerele de luat vederi sunt din ce în ce mai răspândite și la locul de muncă și, deși angajatorul are interese semnificative în operarea unui sistem de camere, nu trebuie uitat că acest fapt vine cu restrângerea unui drept fundamental al omului, astfel încât să fie respectată cerința stabilită de testul proporționalității-necesității. În ceea ce privește limitarea scopului, acesta se referă la documentele Grupului de lucru pentru protecția datelor, în temeiul articolului 29 [38] (denumit în continuare "grupul de lucru") și precizează că, în dreptul maghiar, temeiul juridic al prelucrării este fie acordul asupra prelucrării datelor, fie subiectul sau dispozițiile unui act. Deși angajatorul ar putea avea interes să folosească aparate de fotografiat datorită intereselor sale economice legale, Comisarul a considerat că este alarmant să restrângă pe bază generală drepturile fundamentale ale angajaților, și a subliniat, de asemenea, problema vulnerabilității existențiale. De asemenea, Grupul de lucru a evaluat problema camerei de supraveghere pe baza mai multor documente. Printre acestea, menționez Avizul 8/2001 privind prelucrarea datelor cu caracter personal în contextul ocupării forței de muncă și Avizul 4/2004 privind prelucrarea datelor cu caracter personal prin intermediul supravegherii video. În ambele documente, Grupul de lucru explică faptul că dispozițiile Directivei DPD se aplică monitorizării la locul de muncă. Grupul de lucru a recunoscut că este necesar să se clarifice aplicabilitatea regulamentului privind protecția datelor cu privire la domeniul monitorizării la locul de muncă și la utilizarea camerei de supraveghere. În ceea ce privește subiectul monitorizării la locul de muncă, Grupul de lucru a subliniat problematica consimțământului ca temei juridic al prelucrării și al interacțiunii dintre legea muncii și legea privind protecția datelor [39].

Comisarul a continuat să examineze cazurile [40] privind folosirea camerei de supraveghere la locul de muncă, analizând interesele angajatorului care pot justifica o astfel de monitorizare și în ce condiții. Conform practicii sale, este interzisă operarea camerelor de luat vederi în spații în care se efectuează o muncă constantă (de exemplu, birouri) în scopul monitorizării muncii și a comportamentului angajaților. Este posibilă operarea camerelor în spații unde se efectuează o muncă constantă, atunci când angajații se confruntă cu un pericol real și direct (de exemplu mișcări, locuri de muncă industriale), dar pericolul trebuie să fie real și direct. În cazuri excepționale, este de asemenea posibilă utilizarea camerelor pentru a asigura interesul persoanei (de exemplu, casierul). În scopul protejării proprietății, este posibilă utilizarea camerelor de luat vederi pe coridoare, în încăperi de depozitare și pe drumul care duce la aceste spații. Camerele pot fi de asemenea folosite în spațiile necesare pentru protecție, iar imaginile pot fi înregistrate în perioadele în care nimeni nu ar trebui să fie prezent în mod legal în clădire. Este interesant faptul că nu există niciun acord între cercetătorii maghiari, dacă utilizarea camerelor fără capacități de stocare este considerată prelucrare a datelor [41]. În opinia mea, din considerentul 14 al DPD, aceste dispoziții ar trebui să se aplice și camerelor

de luat vederi care nu au funcții de memorare. Acesta precizează că, în ceea ce privește dezvoltarea tehnologiei, DPD ar trebui să se aplice dispozitivelor care captează, transmit, manipulează, înregistrează, stochează sau comunică sunet și imagine. Nici un scop nu ar trebui să justifice monitorizarea în vestiare, băi și în spații destinate relaxării angajaților în timpul orelor de lucru. Comisarul se referă, de asemenea, la dispozițiile relevante ale Legii privind serviciile de securitate și activitățile anchetatorilor privați, afirmând că, deși nu se referă în mod special la monitorizarea la locul de muncă, din cauza lipsei de lex specialis, acestea au un rol orientativ.

3.3. Practica Autorității

Cu toate că, de la 1 ianuarie 2012, instituția Comisarului a fost înlocuită cu Autoritatea, practica Autorității se bazează pe rezoluțiile Comisarului. În contul său anual, Autoritatea a declarat că cetățenii se adresează acelorași probleme și una dintre aceste probleme este supravegherea camerei [42].

În ceea ce privește folosirea camerei de supraveghere la locul de muncă, un pas imens a avut loc la 23 ianuarie 2013, când Autoritatea a emis o recomandare intitulată "Cerințele de bază privind sistemele electronice de monitorizare la locul de muncă" [43], care se referă în detaliu la supravegherea video. În opinia mea, această recomandare poate fi considerată documentul cel mai important în acest domeniu. Problema acestei recomandări a fost necesară deoarece (Comisarul) și Autoritatea au primit un număr din ce în ce mai mare de cazuri în acest domeniu și, de asemenea, pentru că schimbarea mediului juridic și decizia deja menționată a CJUE au creat un nou mediu juridic, a făcut necesară crearea unei practici uniforme.

În opinia mea, partea cea mai de perspectivă și cea mai nouă este obiectul temeiului legal al procesului. Autoritatea a încălcat practica anterioară, și anume, că prelucrarea se poate baza pe două motive juridice și consideră prelucrarea în lumea muncii ca prelucrare, indiferent de consimțământul angajatului. Pe de o parte, pentru a monitoriza dacă angajatul îndeplinește obligația de a perfecționa munca în conformitate cu instrucțiunile angajatorului, Codul Muncii furnizează angajatorului - dreptul deja examinat - dreptul de a monitoriza, care nu are nevoie de consimțământul angajatului. Acest lucru este în conformitate cu legislația UE, deoarece Grupul de lucru s-a exprimat în mai multe dintre avizele sale că natura voluntară a consimțământului salariatului este discutabilă, astfel încât nu constituie un temei juridic adecvat al prelucrării. Pe de altă parte, CJUE a hotărât, în cauzele sale conexe C 468/10 și C 469/10, că articolul 7 litera (f) din DPD are un efect direct, care în principiu oferă prelucrare bazată pe echilibrarea diferitelor interese. Acest temei juridic poate fi aplicat pentru prelucrarea în termenul de lucru, ceea ce înseamnă că, în anumite cazuri unice, în favoarea intereselor angajatorului, respectând garanțiile prevăzute de regulamentul privind protecția datelor, angajatorul poate limita confidențialitatea angajatului și dreptul la protecția datelor. Este important de menționat că monitorizarea este legală numai dacă este absolut necesară, pentru un motiv rațional direct pentru scopul relației de muncă, nu dăunează demnității umane, nu are scopul de a monitoriza viața privată a angajatului, angajatul a fost informat în mod corespunzător înainte de prelucrare și sunt respectate cerințele de bază privind protecția datelor [44]. Recunoașterea de către Autoritate a efectului direct reprezintă un pas important în ceea ce privește respectarea legislației UE, deși în sine nu este suficientă o înțelegere deplină cu privire la temeiurile legale deja prezentate în Legea privind protecția vieții private.

Pe lângă un temei legal adecvat, trebuie respectate și alte cerințe. Recomandarea subliniază faptul că Codul Muncii încă nu conține prevederi detaliate, deci până la adoptarea unei reglementări speciale prevederile Legii privind serviciile de securitate și activitățile investigatorilor privați au un rol orientativ (singurul act care a fost o referință atât în practica Comisarului, cât și al Autorității, și este încă în vigoare astăzi [45]). Recomandarea subliniază, de asemenea, care sunt scopurile legale pentru utilizarea monitorizării electronice în contextul ocupării forței de muncă. Un scop legitim poate fi, în primul rând, protecția vieții umane și a integrității fizice, libertatea personală, protejarea substanțelor periculoase, protecția afacerilor, plata, secretul bancar și al valorilor mobiliare și protecția proprietății. Aceasta înseamnă că spațiile cu pericol potențial pot fi monitorizate pentru protecția persoanelor (de exemplu, salonul de asamblare). Pentru protecția proprietății, camerele pot fi folosite numai în cazuri justificate în mod corespunzător (în special în încăperi și coridoare în cazul în care sunt necesare protecția instrumentelor, a materiilor prime și a altor obiecte de valoare prețioase stocate la locul de muncă). Monitorizarea are o limită absolută: dreptul la demnitatea umană. Aceasta înseamnă că, camerele nu pot fi folosite pentru a monitoriza activitatea unui anumit angajat sau dacă scopul este de a influența comportamentul la locul de muncă. Este interzisă în mod explicit utilizarea camerelor de luat vederi, de exemplu, în vestiare, dușuri, băi, camere medicale sau în

încăperi destinate relaxării în timpul orelor de lucru. Dacă nimeni nu poate fi prezent, în mod legal, în incinta locului de muncă (în special după orele de lucru și în timpul vacanțelor), fiecare parte a locului de muncă poate fi monitorizată. Cerințele legate de aceste scopuri vor fi aplicate în funcție de unghiul fiecărui aparat foto.

În ceea ce privește stocarea înregistrărilor, Autoritatea a recomandat, ca regulă generală, că imaginile pot fi stocate pentru o perioadă de 3 zile lucrătoare. Angajatorul trebuie să justifice dacă, în cazuri excepționale, este necesară o perioadă mai lungă de depozitare. Dacă sunt îndeplinite anumite condiții speciale, este acceptabil să fie stocate imaginile timp de 30 sau 60 de zile. Există, de asemenea, cerințe privind afișarea înregistrărilor; numai un cerc limitat de persoane poate avea dreptul de a consulta imaginile, numai aceia care, pe baza înregistrărilor, au dreptul să decidă la locul de muncă. De asemenea, se va reglementa cine, în ce scop și cât de des poate consulta înregistrările.

Dreptul la informații preliminare este semnificativ. Informațiile furnizate într-un format scris includ "temeiul legal al prelucrării, amplasarea fiecărei camere și scopurile acestora, zona monitorizată de acestea, subiectul lor, dacă angajatorul operează un sistem de monitorizare directă sau stochează înregistrările, identitatea persoanei (juridice sau naturale) care operează sistemul de monitorizare electronică, unde și pentru cât timp va fi stocată înregistrarea, instrucțiunile de securitate a datelor privind stocarea înregistrărilor, identitatea persoanelor îndreptățite să consulte imaginile și care sunt organizațiile, cazurile în care pot fi transferate înregistrările, regulile de consultare a înregistrărilor, în ce scop angajatorul poate folosi înregistrările, ce drepturi au angajații în ceea ce privește monitorizarea electronică și modul în care le pot exercita, iar în cazul încălcării dreptului lor la autodeterminarea informațională ce fel de aplicare poate să le utilizeze" [46]. Este important că aceste informații trebuie redactate într-un format ușor de înțeles, în cazul în care nu se utilizează nici un jargon. Angajatorul trebuie să justifice că a furnizat informațiile. El va indica, de asemenea, prezența unei astfel de monitorizări cu un semn distinctiv de atenționare [47].

După părerea mea, recomandarea Autorității a rezolvat în mod adecvat problema camerei de supraveghere la locul de muncă, oferind înțeles concret și exact dispozițiilor generale ale Codului Muncii și Legii privind confidențialitatea. În ceea ce privește temeiul juridic al procesării, este un pas imens - indiferent de lipsa modificărilor necesare - că Autoritatea a declarat explicit că articolul 7 litera (f) din DPD are un efect direct și că acest temei juridic se aplică în cazuri de monitorizare a angajaților. În ceea ce privește respectarea legislației UE, trebuie remarcat faptul că, atât Comisarul, cât și Autoritatea [48] au reafirmat de mai multe ori documentele Grupului de lucru, astfel că practica maghiară de protecție a datelor respectă legea UE.

Concluzii

În concluzie, se poate afirma că, recent, legea ungară privind protecția datelor a cunoscut o transformare semnificativă atât în ceea ce privește normele legale, cât și cele instituționale. În timpul acestei transformări, Ungaria a făcut pași în vederea respectării legislației UE și a protecției eficiente a dreptului angajatului la protecția datelor. În timpul înlocuirii regulamentului privind protecția datelor, cea mai importantă modificare a fost legată de temeiurile juridice ale prelucrării. Au existat diferențe semnificative între temeiurile juridice ale DPD și temeiurile juridice definite în actul anterior de protecție a datelor, însă adoptarea Legii privind confidențialitatea este acum mai aproape de cerințele UE. Totuși, legislația are o insuficientă importanță, deoarece actul normativ nu respectă pe deplin legislația UE; conform unei decizii a CJUE din 2011, modificarea actului normativ maghiar va fi necesară pentru a respecta obligația de implementare a DPD. Cealaltă schimbare importantă se referea la protecția instituțională; Comisarul a fost înlocuit de Autoritate, iar această înlocuire a condus la condamnarea de către CJUE.

În domeniul protecției datelor, în contextul ocupării forței de muncă, am putut, de asemenea, să trecem printr-o schimbare uriașă prin intrarea în vigoare a noului Cod al Muncii; acest Cod conține acum dispoziții care reglementează în mod explicit problema monitorizării locurilor de muncă, ceea ce reprezintă un pas uriaș în ceea ce privește dreptul angajatului la protecția datelor. În același timp, nu conține dispoziții detaliate și întrucât există și o lipsă de reglementare sectorială, practica Comisarului și a Autorității oferă un înțeles real și aplicabil acestor dispoziții abstracte în contextul folosirii camerei de supraveghere. Comisarul și Autoritatea examinează în detaliu și în mod explicit problema camerei de supraveghere la locul de muncă, respectând "practica" UE, pentru a reglementa în mod adecvat această problemă în Ungaria.

Referinţe

[1] Supervisors: József HAJDÚ (University of Szeged) and Francis KESSLER (University Paris 1 Panthéon Sorbonne)

[2] WARREN, Samuel D. – BRANDEIS Louis D.: *The Right to Privacy*. Harvard Law Review, Vol. 4, No. 5 (1890) p. 193

[3] HAJDÚ József: *A munkavállalók személyiségi jogainak védelme*. Pólay Elemér Alapítvány, Szeged, 2005, p. 8.

[4] SZABÓ Máté Dániel: *Kísérlet a privacy fogalmának meghatározására a magyar jogrendszer fogalmaival.* Információs Társadalom, Vol. 5. Iss. 2. (2005) p. 46.

[5] JÓRI András: *Adatvédelmi kézikönyv*. Osiris Kiadó, Budapest, 2005, pp. 25-26.

[6] HALMAI Gábor –TÓTH Gábor Attila: *Emberi jogok*. Osiris Kiadó, Budapest, 2008, p. 584.

[7] Subsection (1) of Article I of the Fundamental Act

[8] Although these decisions were adopted in a different legal era, the Constitutional Court stated that due to the similar content of the two constitutions' dispositions, the referral to these decisions is still possible in some cases. See more: decision No. 22/2012. (V. 11.) and decision No. 13/2013. (VI. 17.)

[9] On the subject of the personality rights in the Civil Code see more in: VÉKÁS Lajos (ed.): *Az új Polgári Törvénykönyv magyarázatokkal*. Complex Kiadó, Budapest, 2013, pp. 55-68. and WELLMANN György (ed.): *Polgári jog. Bevezető és záró rendelkezések, az ember mint jogalany, öröklési jog.* HVG-ORAC Lap- és Könyvkiadó Kft., Budapest, 2014, pp. 166-198.

[10] CSEH Gergely: *Kamerás megfigyelés a munkahelyeken – avagy milyen párhuzamok és ellentétek figyelhetők meg az adatvédelmi biztos és a Hatóság gyakorlata között.* Miskolci Jogi Szemle, Vol. 9. Iss. 2. (2014) p. 12.

[11] The Hungarian National Authority for Data Protection and Freedom of Information Summary Report 2012, p. 13.

[12] BALOGH Zsolt György – POLYÁK Gábor – RÁTAI Balázs – SZŐKE Gergely László: *Munkahelyi adatvédelem a gyakorlatban.* Infokommunikáció és Jog, No. 50. (2012) p. 97.

[13] PÉTERFALVI Attila (ed.): *Adatvédelem és információszabadság a mindennapokban*. HVG-ORAC, Budapest, 2012, pp. 106-107.

[14] C-468/10 ASNEF (ECLI:EU:C:2011:777)

[15] See for example: Article 29 Data Protection Working Party: *Opinion 8/2001 on the processing of personal data in the employment context*. 5062/01/EN/FinalWP 48, 2001, p. 23.; Commissioner case number: 1165/K/2005-3.

[16] HALMAI – TÓTH 2008, p. 592.

[17] JÓRI 2005, p. 136.

[18] Sections 7-8 and Sections 14-22 of the Privacy Act

[19] C-288/12 Commission v Hungary (ECLI:EU:C:2014:237) par. 59-62

[20] BALOGH – POLYÁK– RÁTAI– SZŐKE 2012, p. 99.

[21] KARDKOVÁCS Kolos (ed.): *A Munka Törvénykönyvének magyarázata. Harmadik, hatályosított kiadás.* HVG-ORAC Lap-és Könyvkiadó Kft., Budapest, 2016, p. 52.

[22] CSÉFFÁN József: *A Munka Törvénykönyve és magyarázata*. Szegedi Rendezvényszervező Kft, Szeged, 2014, p. 44.

[23] KARDKOVÁCS (ed.) 2016, p. 136.

[24] VITALIS, André: *Kamerás megfigyelés, biztonság és szabadságjogok*. Információs Társadalom, Vol. 2. Iss. 1. (2002) pp. 56-57.

[25] See: VITALIS 2002, pp. 58-59.; GALÁNTAI Zoltán: *E-privacy olvasókönyv*. Available at: http://mek.oszk.hu/04100/04134/html/ (Accessed: 2 November 2016)

[26] SZŐKE Gergely László (ed.): *Privacy in the workplace. Data protection law and self-regulation in Germany and in Hungary*. HVG-ORAC Lap- és könyvkiadó, Budapest, 2012, p. 237.

[27] PERSSON, Anders J. – HANSSON, Sven Ove: *Privacy at Work – Ethical Criteria.* Journal of Business Ethics, Vol. 42. Iss. 1. (2003) p. 65.

[28] See more: Sections 166-176 of the Act I of 2012 on the Labour Code, Act XCIII of 1993 on workplace safety

[29] MILLER, Seumas – WECKERT, John: *Privacy, the Workplace and the Internet.* Journal of Business Ethics, Vol. 28. Iss. 3. (2000) p. 260.

[30] GYULAVÁRI Tamás (ed.): *Munkajog*. Budapest, 2013, ELTE Eötvös Kiadó, p. 244.

[31] HAJDÚ 2005, p. 20.

[32] KARDKOVÁCS (ed.) 2016, pp. 134-138.

[33] Subsection (2) of Section 2 and Sections 60-61 of the Act XCIII of 1993

[34] HAJDÚ 2005, p. 20.

[35] SZÉKELY Iván – SZABÓ Máté Dániel: *A privacy védelme a munkahelyen.* In: Székely Iván – Szabó Máté Dániel (ed.): Szabad adatok – védett adatok. Budapesti Műszaki Egyetem Információ- és Tudásmenedzsment Tanszék, Budapest, 2005, p. 126.

[36] BALOGH – POLYÁK– RÁTAI– SZŐKE 2012, p. 97.

[37] SZŐKE (ed.) 2012, p. 102.

[38] Article 29 Data Protection Working Party: *Opinion 8/2001 on the processing of personal data in the employment context*. 5062/01/EN/FinalWP 48, 2001 and Article 29 Data Protection Working Party: *Working document on the surveillance of electronic communications in the workplace*. 5401/01/EN/FinalWP 55, 2002.

[39] "*The EDPS video-surveillance guidelines"* issued by the European Data Protection Supervisor (EDPS) on the 17 March 2010 and its follow up report should also be mentioned. In these documents the EDPS provided a detailed analysis and explanation to the EU institutions and bodies on how video surveillance can be implemented. (Available: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/12-02-13_Report_CCTV_EN.pdf, Accessed : 23 May 2016)

[40] Commissioner case number: 1805/A/2005-3.; 598/P/2007-8.; 666/P/2008-3.; 368/P/2009-6.; 2812/P/2009-6.; 2900/P/2009-3.

[41] See for example: Commissioner case number: 475/H/2000; 1099/A/2006-6; 666/P/2008-3.; Authority case number: NAIH- 4384-2/2012/V

[42] *Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója* 2012, p. 25.

[43] Authority case number: NAIH-4001-6/2012/V

[44] Authority case number: NAIH-4001-6/2012/V

[45] CSEH 2014, p. 156.

[46] Authority case number: NAIH-4001-6/2012/V, p. 7.

[47] See more: ARANY-TÓTH Mariann: *Személyes adatok kezelése a munkaviszonyban*. Wolters Kluwer, Budapest, 2016, pp. 81-106. and *Annual report of the National Authority for Data Protection and Freedom of Information (NAIH) 2012*, National Authority for Data Protection and Freedom of Information Budapest, 2013, pp. 22-24.

[48] Commissioner case number: 1165/K/2005-3.; Authority case number: NAIH-4001-6/2012/V

= ISSN 2285-0171 ISSN-L=2285-0171